(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 June 2003 (12.06.2003)

PCT

(10) International Publication Number
WO 03/049042 A1

(51) International Patent Classification[7]: G07C 9/00

(21) International Application Number: PCT/CA01/01736

(22) International Filing Date: 6 December 2001 (06.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/078,396 (CIP)
Filed on 13 May 1998 (13.05.1998)

(71) Applicant *(for all designated States except US)*: **BIO-SCRYPT INC.** [CA/CA]; Suite 500, 5450 Explorer Drive, Mississauga, Ontario L4W 5M1 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HOLLINGSHEAD, Dennis, W.** [CA/CA]; Suite 200, 1220 Sheppard Avenue East, Toronto, Ontario M2K 2S5 (CA).

(74) Agent: **FETHERSTONHAUGH & CO.**; Attention: Ronald d. Faggetter, Suite 1500_Box 111, 438 University Avenue, Toronto, Ontario M5G 2K8 (CA).

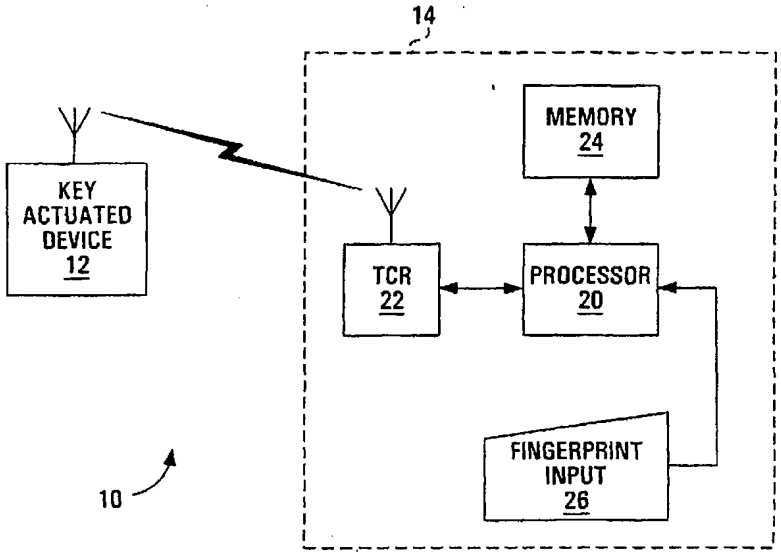
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PORTABLE DEVICE AND METHOD FOR ACCESSING DATA KEY ACTUATED DEVICES



(57) Abstract: Data key actuated devices such as high security doors are modified so that they periodically transmit an identity pattern. An authorized user is provided with a portable access device storing keys for a number of such key actuated devices, with each key associated with an identity pattern for that device. The portable access device has a stored template comprising a fingerprint of the authorized user combined with a verification code. When the authorized user applies their fingerprint to the portable access device, the verification code is returned which allows verification of the user. If the access device then receives a key actuated device identifier matching one in storage, the associated access key is retrieved and transmitted to the key actuated device to allow access to the user.

WO 03/049042 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PORTABLE DEVICE AND METHOD FOR ACCESSING DATA KEY ACTUATED DEVICES

FIELD OF THE INVENTION

This invention relates to a method for accessing data key actuated devices, a portable device for accessing such key actuated devices, and a secure access system.

BACKGROUND OF THE INVENTION

Access to an increasing number of devices is controlled by data access keys. For example, access to an automated teller machine (ATM) is controlled by keypad entry of an appropriate personal identification number (PIN). Similarly, access to high security doors may be controlled by keypad entry of a pass code. Access to security systems, computer networks, and voice mail systems are also typically pass code controlled. As the number of devices which demand an access key for access increases, it becomes more difficult for a user to recall all the necessary access keys. Furthermore, the security of such key actuated devices may be compromised if the access key is not maintained in strict secrecy by the authorized user.

This invention seeks to overcome drawbacks of known security systems.

SUMMARY OF THE INVENTION

According to the present invention, there is provided a method for accessing data key actuated devices, comprising: receiving a key actuated device identifier from a key actuated device; receiving a biometric; determining whether said received biometric is an authorized biometric; comparing said received key actuated device identifier with stored key actuated device identifiers and, on finding a matching stored key actuated device identifier and where said received biometric is an authorized biometric, retrieving a stored access key

associated with said matching stored key actuated device identifier; and transmitting said retrieved access key.

According to another aspect of the invention, there is provided a portable electronic access device comprising: a biometric input; a verifier responsive to said biometric input for verifying that a biometric which is input to said biometric input matches an authorized biometric and providing a verification indication; a memory storing a plurality of access keys, each for use in accessing a key actuated device and a plurality of key actuated device identifiers, each associated with one of said plurality of access keys; a receiver for receiving a key actuated device identifier; a comparator for, responsive to a verification indication from said verifier, comparing a key actuated device identifier received from a key actuated device with said stored key actuated device identifiers and, on finding a matching stored key actuated device identifier, retrieving a stored access key associated with said matching stored key actuated device identifier; and a transmitter for transmitting a retrieved access key.

BRIEF DESCRIPTION OF THE DRAWINGS

In the figures which illustrate an example embodiment of the invention,

figure 1 is a block diagram of a secure access system made in accordance with this invention, and

figure 2 is a flow diagram for operation of the process of figure 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Turning to figure 1, a secure access system 10 comprises a data key actuated device 12 and a portable key access device 14. The key actuated device 12 could be a high security (vehicle or installation) door, an ATM, a security system, a computer network, a voice mail system or any other device requiring a data key for access. The key access device 14 comprises a processor 20 connected for two-way communication with a transceiver 22 and for

two-way communication with a memory 24. The processor also receives signals from fingerprint input 26. Memory 24 is non-volatile and stores a plurality of access keys each for use in accessing a key actuated device. The memory also stores a plurality of key actuated device identifiers, each associated with one of the plurality of stored access keys. The transceiver 22 is wireless and may communicate with the key actuated device via radio transmissions or infrared transmissions. The key access device 14 is portable and preferably battery powered. A switch (not shown) may disconnect the battery when the device is not in use to conserve battery power.

In order to use the portable access device, a user must first be enrolled. To effect enrolment, the user must pass a digitized copy of their fingerprint to an enrolment computer. This may be accomplished by the user applying their finger to the fingerprint input 26 of the access device 14 when the device is connected via a port (not shown) to the enrollment computer so that the processor 20 of the access device is prompted to pass along the digitized fingerprint image to the enrollment computer. Alternatively, the user may apply their fingerprint directly to a fingerprint input associated with the enrolment computer. This computer then calculates a template from the user's fingerprint which is an encrypted combination of the fingerprint with a verification code. Suitable techniques for obtaining such templates from a fingerprint and a code, and for recovering a code from such a template, are described in U.S. patent No. 5,680,460 entitled BIOMETRIC CONTROLLED KEY GENERATION to Tomko et al., the contents of which are incorporated by reference herein. This template is then downloaded to the portable access device and stored in memory 24. Further, the enrolment computer stores a verification indication at an address in memory 24 indicated by the verification code. Enrollment is then completed.

Operation of the system 10 of figure 1 is described in conjunction with figure 1 along with figure 2, which illustrates program control for processor 20. Key actuated device 12 periodically transmits a device identifier. It is generally preferred that the time between such transmissions is no more than about five seconds; the range of these transmissions is preferably about two meters. When the portable access device 14 is brought within range of the transmissions of the key actuated device and is turned on, transceiver 22 will receive these transmissions and pass along the key actuated device identifier to processor 20 (block 50). If

the user of the portable access device then applies their fingerprint to fingerprint input 26, the fingerprint image is also received by processor 20 (block 52).

The processor may then determine whether the fingerprint which was input is that of the authorized user. This is accomplished by the processor retrieving the template stored in memory 24 on enrollment and combining this with the newly input fingerprint from input 26. The resulting verification code is used as a memory address to memory 24. If the processor finds a verification indication at this memory address in memory 24, then the biometric is considered to be authorized (block 54). In such case, the processor compares the received key actuated device identifier with key actuated device identifiers in memory. On a match being found (block 56) the processor passes a valid user indication to transceiver 22 for transmission to the key actuated device 12 (block 58). This valid user indication could comprise the verification code, or an encrypted version of same. Additionally, the processor retrieves the access key from memory 24 which is associated with the matching key actuated device identifier (block 60).

When the key actuated device 12 receives a valid user indication from access device 14, it transmits a one time temporary encryption key. This is received by transceiver 22 and passed to processor 20. Processor 20 uses the temporary key to encrypt the retrieved access key (block 62). The encrypted access key is then passed to the transceiver 22 and transmitted to the key actuated device (block 64). The key actuated device uses a decryption key to recover the decrypted access key and, if the resulting decrypted key is a valid key, allows access to the user. Where the key actuated device is a high security door, this results in the door being unlocked. Where the key actuated device is an ATM, this would allow the user access to the device via a keypad which could be provided on the portable access device 14.

It will be apparent that since the access device 14 stores a number of key actuated device identifiers and associated access keys, device 14 may be carried around by an authorized user and used to gain access to a number different key actuated devices without need of the user to memorize a plurality of pass codes.

The portable access device may be used with an existing key actuated device by modifying the device to incorporate a transceiver in same and programming the processor of the key actuated device so that the device functions in the manner described.

A number of modifications to the system as described are possible. For example, the valid user ID may be transmitted as soon as an authorized fingerprint is received by the access device 14 in advance of determining whether the received key actuated device identifier matches one of the stored identifiers.

Optionally, for lower security applications, the portable access device does not transmit a valid user indication, nor does the key actuated device transmit any temporary keys. Instead, for such applications, on access device 14 determining that an authorized user has applied their fingerprint to the input and on finding an access key for the key actuated device, this access key is transmitted in unencrypted form to the key actuated device.

Another option is for the key actuated device 12 to send a "medium security" indicator when it wants the access device 14 to send a verification code and receive a temporary key for encrypting the access keys prior to transmission and to send a "low security" indicator, or no security indicator, when it wants the access device 14 to follow the described low security option.

A high security option is for the access keys to be encrypted in the access device 14. To accomplish this option, on enrolment, as well as forming a template from the user's fingerprint and a verification code, a template is formed from the user's fingerprint and a special key. The special key is then used to encrypt each access key. In operation, when the access device 14 receives a key actuated device identifier and a user's fingerprint, it retrieves any associated encrypted access key and both templates. If the fingerprint is that of the authorized user, the fingerprint successfully returns the verification code from the one template. This results in the access device 14 sending a verification indication to the key actuated device 12. The key actuated device responds by sending a temporary encryption key. The access device then uses the fingerprint to return the special key from the other fingerprint template and the special key is then used to decrypt the access key. The access device 14 next

uses the temporary key to encrypt the access key and sends the encrypted access key to the key actuated device 12.

It will be obvious to those skilled in the art that the transmission of the retrieved access key may be protected by other cryptographic means. For example, a Public Key Infrastructure (PKI) may be used, such that the retrieved access key is first digitally signed using the private key of the user (synonymous with the special key above), and then encrypted using the public key of the key actuated device (synonymous with the temporary key above). This encrypted data package is then sent to the key actuated device. The user can thus be assured that only the appropriate authority can properly use the transmitted data (as only they have the private key of the key actuated device to decrypt the data), and the key actuated device can correspondingly ensure that the authorized user was present (by verifying the digital signature of the retrieved access key using the public key of the user). This provides strong mutual authentication between the actual user of the system and the key actuated device (rather than only between the portable access device and the key actuated device), as the digital signature can only be initiated subsequent to the user providing positive biometric authentication. This embodiment provides for not only a secure transmission line between the electronic access device and the key actuated device, but also provides a high degree of transaction accountability as the user must be present to initiate digital signing.

Other methods for the secure transmission of the retrieved access key will be obvious to those skilled in the art.

While in the described embodiment the user is authorized solely at the portable access device, it would be possible for the key actuated device to participate in this authorization. More particularly, on enrolment, the enrolment computer could simply pass the template to the portable access device and not the verification indication. In such instance, when a biometric is input to the access device, a verification code is returned and this code is passed directly (in encrypted or unencrypted form) to the key actuated device. The key actuated device could then pass the code to a central database which would use it to look up whether the code was indicative of a valid user. If so, the key actuated device would prompt

the access device to continue. Further the key actuated device would only respond to any key transmitted by the access device where the key actuated device determined the user was authorized.

In circumstances where the access device is to transmit a valid user indication and the key actuated device is to respond with a temporary key, the valid user indication is conveniently the (encrypted or unencrypted) recovered verification code and the prompt from the key actuated device is conveniently the temporary key.

While device 14 is shown for use with a fingerprint input, equally any other user biometric could be employed. For example, access device 14 could scan an iris of a user.

Since any biometric verification device will have a non-zero false acceptance rate, preferably the key access devices 14 is programmed to shut down or broadcast an alarm code after a pre-determined number of consecutive failed verification attempts by a user.

Other modifications will be apparent to those skilled in the art and, therefore, the invention is defined in the claims.

WHAT IS CLAIMED IS:

1. A method for accessing data key actuated devices, comprising:

receiving a key actuated device identifier from a key actuated device;

receiving a biometric;

determining whether said received biometric is an authorized biometric;

comparing said received key actuated device identifier with stored key actuated device identifiers and, on finding a matching stored key actuated device identifier and where said received biometric is an authorized biometric, retrieving a stored access key associated with said matching stored key actuated device identifier; and

transmitting said retrieved access key.

2. The method of claim 1 further comprising:

receiving a temporary key; and

encrypting said retrieved access key with said temporary key prior to transmission of said retrieved access key.

3. The method of claim 2 further comprising:

responsive to determining said received biometric is an authorized biometric, initially transmitting a valid user indication.

4. The method of claim 3 wherein said temporary key is received subsequent to transmitting said valid user indication.

5. The method of claim 3 or claim 4 wherein said initially transmitting a valid user indication is dependent upon finding a stored key actuated device identifier matching said received key actuated device identifier.

6. The method of any of claims 2 to 5 wherein each said stored access key is encrypted and including performing a decryption operation on a retrieved access key prior to encrypting said retrieved access key with said temporary key.

7. The method of claim 6 wherein each said stored access key is encrypted with a special key and wherein said performing a decryption operation comprises retrieving a template and attempting to recover said special key from said template utilizing said received biometric.

8. The method of any of claims 1 to 6 further comprising retrieving a template and attempting to recover a special key from said template utilizing said biometric, said special key for use in performing a cryptographic operation.

9. The method claim 8 wherein said cryptographic operation involves at least one said access key.

10. The method of any of claims 3 to 5 wherein said initially transmitting a valid user indication is dependent upon finding a stored key actuated device identifier matching said received key actuated device identifier.

11. The method of any of claims 1 to 10 wherein said determining whether said received biometric is an authorized biometric comprises utilizing a template comprising said authorized biometric and a verification code such that presence of said biometric allows recovery of said verification code.

12. A portable electronic access device comprising:

a biometric input;

a verifier responsive to said biometric input for verifying that a biometric which is input to said biometric input matches an authorized biometric and providing a verification indication;

a memory storing a plurality of access keys, each for use in accessing a key actuated device and a plurality of key actuated device identifiers, each associated with one of said plurality of access keys;

a receiver for receiving a key actuated device identifier;

a comparator for, responsive to a verification indication from said verifier, comparing a key actuated device identifier received from a key actuated device with said stored key actuated device identifiers and, on finding a matching stored key actuated device identifier,

retrieving a stored access key associated with said matching stored key actuated device identifier; and

a transmitter for transmitting a retrieved access key.

13. The device of claim 12 wherein said stored access keys are encrypted and including a decrypter for decrypting a retrieved access key prior to said access key being transmitted by said transmitter.

14. The device of claim 12 wherein said memory is also for storing a special key template, said access keys are encrypted with a special key and said decrypter is responsive to said biometric input to perform a special key recovery operation on said special key template utilizing said input biometric and a subsequent decrypting operation on said retrieved access key utilizing a recovered special access key.

15. The device of claim 12 or claim 13 wherein said memory is also for storing a special key template comprising said authorized biometric and a special key, said special key for use in performing a cryptographic operation.

16. The device of any of claims 12 to 15 wherein said verifier is for accessing a stored template comprising said authorized biometric and a verification code, for attempting to recover said verification code from an input biometric and for using said verification code to obtain said verification indication.

17. The device of any claims 12 to 16 wherein said receiver is also for receiving a temporary key and including an encrypter for encrypting said retrieved access key with said temporary key prior to transmission of said retrieved access key by said transmitter.

18. The device of any of claims 12 to 17 wherein said transmitter is also for initially transmitting a valid user indication in response to said verifier providing said verification indication.

19. The device of claim 17 wherein said transmitter is also for initially transmitting a valid user indication in response to said verifier providing said verification indication and wherein said temporary key is received after said transmitter has transmitted said valid user indication.

20. The device of any of claims 12 to 19 wherein said receiver comprises one of a radio receiver and an infrared receiver and said transmitter comprises one of a radio transmitter and an infrared transmitter.

21. A secure access system, comprising:

a data key actuated device for periodically transmitting a key actuated device identifier;

a portable access device comprising:

a biometric input;

a verifier responsive to said biometric input for verifying that a biometric which is input to said biometric input matches an authorized biometric and providing a verification indication;

a memory storing a plurality of access keys, each for use in accessing a key actuated device and a plurality of key actuated device identifiers, each associated with one of said plurality of access keys;

a receiver for receiving said key actuated device identifier;

a comparator for, responsive to a verification indication from said verifier, comparing a key actuated device identifier received from said key actuated device with said stored key actuated device identifiers and, on a match, retrieving an access key associated with said matching stored key actuated device identifier; and

a transmitter for transmitting a retrieved access key to said key actuated device.

22. The system of claim 21 wherein said receiver is for receiving a temporary key and wherein said access device includes an encrypter for encrypting said retrieved access key with said temporary key prior to transmission of said retrieved access key by said transmitter.

23. The system of claim 21 or 22 wherein said transmitter is also for initially transmitting a valid user indication in response to said verifier providing said verification indication to said access device and wherein said key actuated device is also for, responsive to receiving said

valid user indication, transmitting said temporary key.

24. The system of any of claims 21 to 23 wherein said memory is also for storing a template and wherein said verifier is also for attempting to recover a special key from said template utilizing said biometric, said special key for use in performing a cryptographic operation.

25. The system of any of claims 21 to 24 wherein wherein said transmitter is a radio transmitter and said receiver is a radio receiver.

26. The system of any of claims 21 to 25 wherein said verifier is for accessing a stored template comprising said authorized biometric and a verification code, for attempting to recover said verification code from an input biometric and for using said verification code to obtain said verification indication.

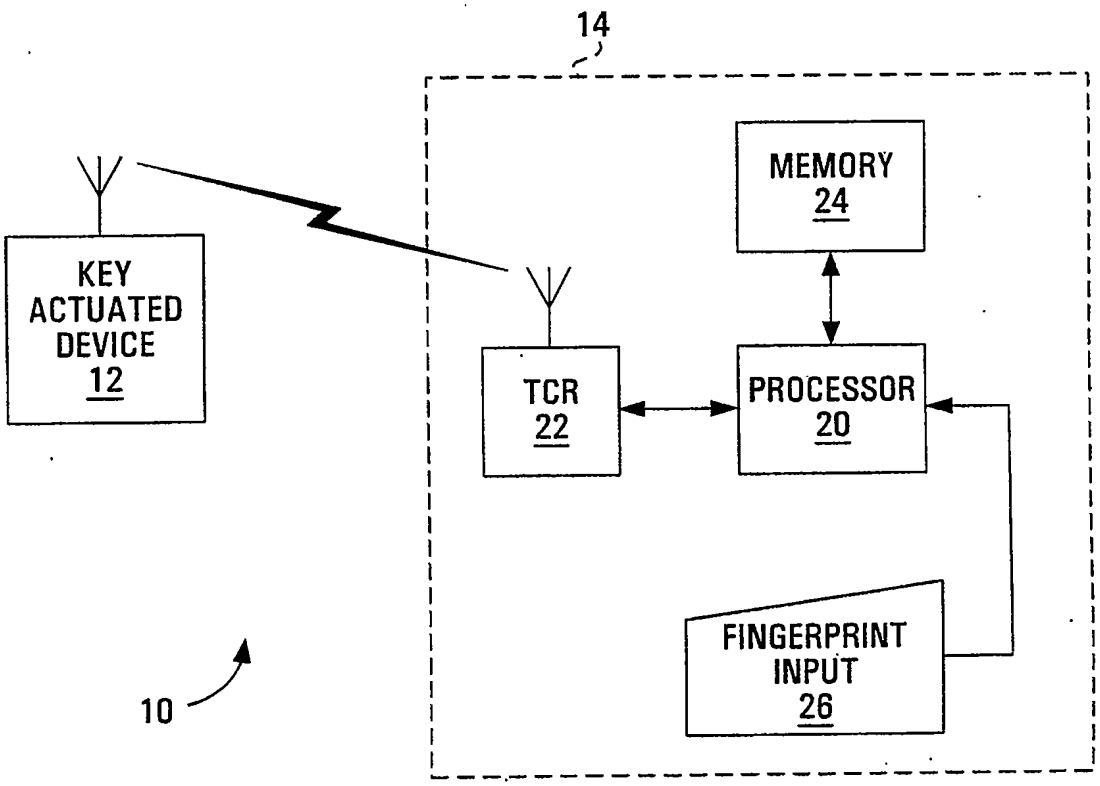

14
MEMORY
24
KEY
ACTUATED
DEVICE
12
TCR
22
PROCESSOR
20
FINGERPRINT
INPUT
26
10

FIG. 1

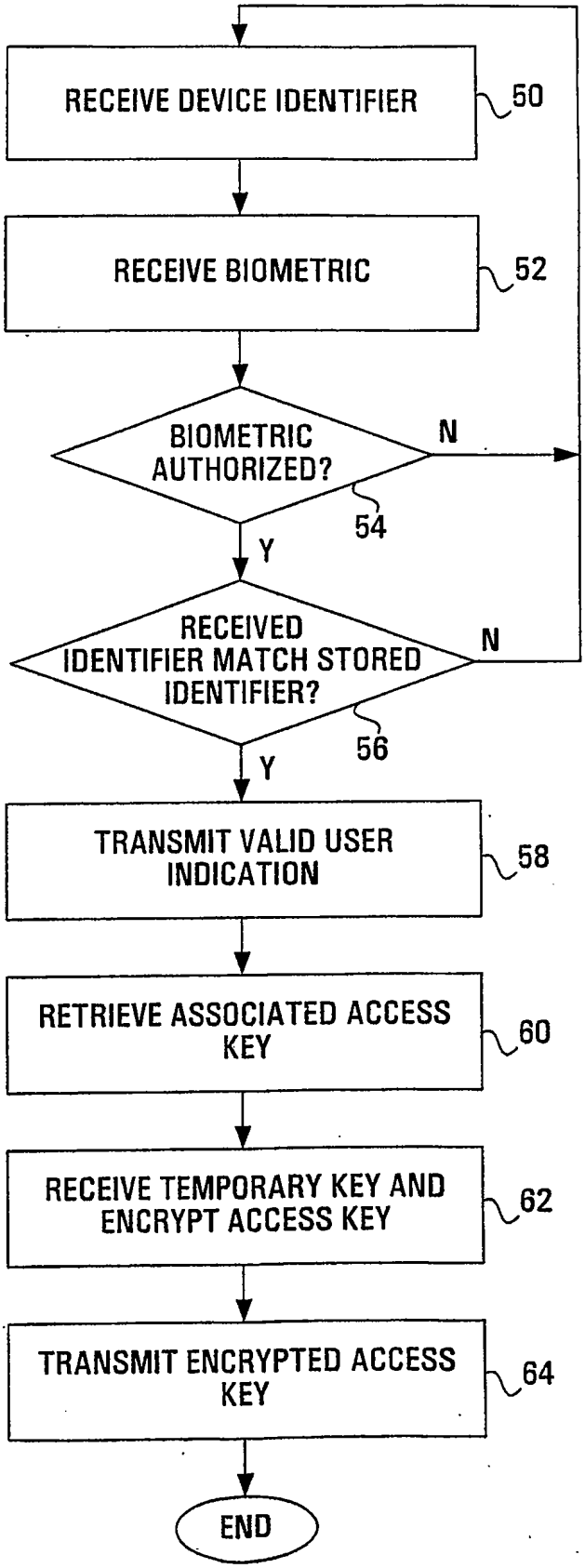

RECEIVE DEVICE IDENTIFIER
50
RECEIVE BIOMETRIC
52
BIOMETRIC AUTHORIZED?
N
54
Y
RECEIVED IDENTIFIER MATCH STORED IDENTIFIER?
N
56
Y
TRANSMIT VALID USER INDICATION
58
RETRIEVE ASSOCIATED ACCESS KEY
60
RECEIVE TEMPORARY KEY AND ENCRYPT ACCESS KEY
62
TRANSMIT ENCRYPTED ACCESS KEY
64
END

FIG. 2

INTERNATIONAL SEARCH REPORT

national Application No
PCT/CA 01/01736

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G04C G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 924 657 A (TRW INC) 23 June 1999 (1999-06-23)	1
A	paragraph '0017! - paragraph '0031!	2-4,11, 12,17-23
Y	US 5 131 038 A (CANTARUTTI TRACEY L ET AL) 14 July 1992 (1992-07-14)	1
A	column 3, line 45 -column 5, line 45 column 6, line 15 - line 26 claim 1	12,20, 21,25

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 May 2002	03/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bocage, S

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

national Application No
PCT/CA 01/01736

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 12670 A (BORZA STEPHEN J ;FREEDMAN GORDON (CA); DEW ENGINEERING AND DEV LIM) 26 March 1998 (1998-03-26) page 7, line 27 -page 9, line 2 page 12, line 10 - line 25 page 16, line 5 - line 27 page 19, line 22 -page 20, line 2 ---	12
A	GB 2 181 582 A (BLACKWELL VICTOR CAMPBELL) 23 April 1987 (1987-04-23) page 3, line 9 -page 4, line 9 claims 2,4,5,8 ---	1
A	EP 0 869 460 A (PITNEY BOWES) 7 October 1998 (1998-10-07) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 01/01736

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0924657 A	23-06-1999	US 6038666 A	14-03-2000
		EP 0924657 A2	23-06-1999
		JP 3222111 B2	22-10-2001
		JP 11316818 A	16-11-1999
		US 6182221 B1	30-01-2001
US 5131038 A	14-07-1992	NONE	
WO 9812670 A	26-03-1998	AU 4196497 A	14-04-1998
		CA 2233942 A1	26-03-1998
		WO 9812670 A1	26-03-1998
GB 2181582 A	23-04-1987	AU 6476786 A	05-05-1987
		EP 0241504 A1	21-10-1987
		WO 8702491 A1	23-04-1987
EP 0869460 A	07-10-1998	US 6131090 A	10-10-2000
		EP 0869460 A2	07-10-1998